TECHNIQUE T833: MODIFY CONTROL LOGIC

CyOTE Use Case(s)	MITRE ATT&CK for ICS® Tactic
Alarm Logs, HMI	Inhibit Response Function, Impair Process Control
Data Sources	
Potential Data Sources	Alarm Logs, HMI Data, Network Captures, Firewall Logs, Host Logs, Hashes of Control Logic Payload, VPN Logs, Log-In Activity, Event Records
Historical Attacks	Triton Attack at Petro Rabigh[1]

TECHNIQUE DETECTION

The Modify Control Logic technique[2] (Figure 1) may be detected when there are indications of modified device control logic found in logs from the Potential Data Sources identified above.

To augment commercial sensor gaps, the CyOTE program has developed capabilities such as Proof of Concept tools[3] and Recipes[4] for asset owners and operators (AOO) to identify indicators of attack for techniques like Modify Control Logic within their operational technology (OT) networks. Referencing CyOTE Case Studies[5] of known attacks, AOOs in both small and large organizations can utilize CyOTE's Use Case analyses to tie operational anomalies and observables to cyber-attack campaigns resulting in ever-decreasing impacts.

PERCEPTION: OBSERVABLES FROM HISTORICAL ATTACKS

The Modify Control Logic technique was used in the Triton attack at Petro Rabigh in 2017.[6] In this attack, the following observables were identified:

- Increased internet traffic
- Increased DMZ traffic between information technology (IT) and OT networks

[1] MITRE, *Software: Triton, TRISIS, HatMan,* https://collaborate.mitre.org/attackics/index.php/Software/S0013

[2] MITRE ATT&CK for ICS, T833: Modify Control Logic, https://collaborate.mitre.org/attackics/index.php/Technique/T0833. Note that this technique has been deprecated, and its content merged into T889, Modify Program: https://collaborate.mitre.org/attackics/index.php/Technique/T0889

[3] A Proof of Concept tool is a representative implementation of a set of steps and methods for identifying techniques. A Proof of Concept tool is defined as a script(code) or using capabilities of existing tools (e.g., Splunk, Gravwell), to demonstrate the capability to identify adversarial activity for a selected technique. A Proof of Concept tool is not ready for implementation in an AOO's environment as its major focus is to a specific instance (device, vendor, protocol, scenario) in order to prove a concept.

[4] A Recipe is a set of steps and methods for identifying techniques. Recipes can be used to develop a Proof of Concept or operational tool in an AOO's OT environment.

[5] Visit https://inl.gov/cyote/ for all CyOTE Case Studies.

[6] https://www.eenews.net/stories/1060123327

Disclaimer: Past occurrences are not guaranteed to occur in future attacks.

COMPREHENSION

In the Triton attack at Petro Rabigh, the adversary modified device logic as part of their execution of the attack after having moved into the OT network. They first gained access through an engineering workstation to deploy the malware; once they gained control of the workstation, they modified operating modes on devices and modified device logic to issue malicious command messages and shut down part of the plant.[7] By understanding the nature and possible origins of this attack, as well as how the adversary used the Modify Control Logic technique to execute the attack, an AOO can better comprehend how this technique is used with others and enhance their capabilities to detect attack campaigns using this technique and decrease an attack's impacts.

CURRENT CAPABILITY

The CyOTE Recipe outlines a process to analyze OT network traffic and use deep packet inspection to identify potential indicators arising from an attempt to modify control logic.

POTENTIAL ENHANCEMENTS

Further development may leverage host logs to trigger network traffic capture and assist network capture analysis.

ASSET OWNER DEPLOYMENT GUIDANCE

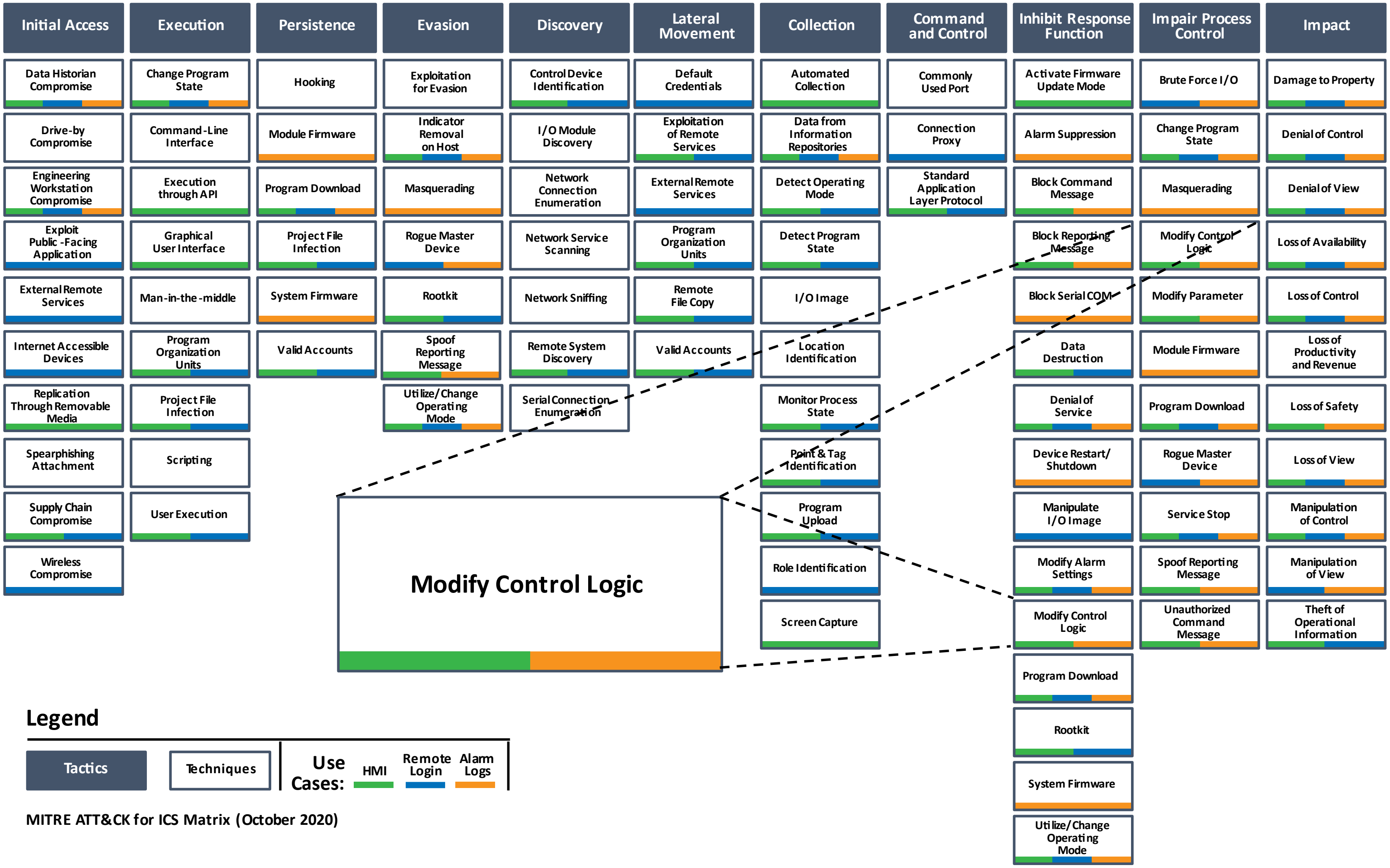
The process in the CyOTE Recipe should be leveraged to develop an operational tool. This tool should be deployed by a network team, in conjunction with cyber defenders and operators, to a host capable of processing the desired amount of traffic in an acceptable time frame. This host will either need access to a span port for live traffic or stored Packet Capture (PCAP) files awaiting to be processed. The operational tool can be configured and populated with supporting information regarding approved hosts.

AOOs can refer to the CyOTE Technique Detection Capabilities report (visit https://inl.gov/cyote/) for more information on the background and approach of CyOTE's technique detection capabilities.

AOOs can also refer to the CyOTE methodology for more information on CyOTE's approach to identifying anomalies in an OT environment, which, when perceived, initiates investigation and analysis to comprehend the anomaly.

Click for More Information	CyOTE Program || Fact Sheet || CyOTE.Program@hq.doe.gov
DOE Senior Technical Advisor	Edward Rhyne || Edward.Rhyne@hq.doe.gov || 202-586-3557

[7] CyOTE Case Study: Triton in Petro Rabigh. https://inl.gov/wp-content/uploads/2021/09/Triton-CyOTE-Case-Study.pdf



Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man-in-the-middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Devices	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/ Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View
						Screen Capture		Modify Control Logic	Unauthorized Command Message	Theft of Operational Information
								Program Download		
								Rootkit		
								System Firmware		
								Utilize/Change Operating Mode		

Figure 1: ICS ATT&CK Framework[8] – Modify Control Logic Technique

[8] © 2020 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.